

DERWENT-ACC-NO: 1996-173962

DERWENT-WEEK: 199618

COPYRIGHT 1999 DERWENT INFORMATION LTD

TITLE: Software for protecting electronic
computer from inaccurate program and computer virus
- detects invalid program by comparing inaccurate
program with program with doubt of inaccurate program infection

PATENT-ASSIGNEE: MASAOKA K[MASAI]

PRIORITY-DATA: 1994JP-0207896 (July 27, 1994)

PATENT-FAMILY:

| PUB-NO | PAGES | PUB-DATE | MAIN-IPC | |
|---------------|-------|-------------------|-------------|-----|
| LANGUAGE | | | | |
| JP 08044556 A | 004 | February 16, 1996 | G06F 009/06 | N/A |

APPLICATION-DATA:

| PUB-NO | APPL-DATE | APPL-DESCRIPTOR | APPL-NO |
|----------------|-----------|-----------------|---------|
| JP 08044556A | | | |
| 1994JP-0207896 | | N/A | |
| | | July 27, 1994 | |

INT-CL (IPC): G06F009/06, G06F012/14

ABSTRACTED-PUB-NO: JP 08044556A

BASIC-ABSTRACT:

The software involves the omission of an inaccurate program, computer virus which enters the memory of an electronic computer. The inaccurate program performs inaccurate operation which are not expected by the user by monitoring the write-in operation and comparing the inaccurate program (2) with program (3) with doubt of inaccurate program infection. The inaccurate program is identified and removed.

ADVANTAGE - Prevents destruction of memory. Prevents invalid operations.

CHOSEN-DRAWING: Dwg.2/2

TITLE-TERMS: SOFTWARE PROTECT ELECTRONIC COMPUTER
INACCURACIES PROGRAM COMPUTER
VIRUS DETECT INVALID PROGRAM COMPARE
INACCURACIES PROGRAM PROGRAM
INACCURACIES PROGRAM INFECT

DERWENT-CLASS: T01

EPI-CODES: T01-F06; T01-H01C; T01-J12C;

SECONDARY-ACC-NO:

Non-CPI Secondary Accession Numbers: N1996-146056

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平8-44556

(43)公開日 平成8年(1996)2月16日

(51)Int.Cl.⁸

G 0 6 F 9/06
12/14

識別記号

5 5 0 Z 7230-5B
3 1 0 Z

府内整理番号

F I

技術表示箇所

審査請求 未請求 請求項の数15 書面 (全 4 頁)

(21)出願番号

特願平6-207896

(22)出願日

平成6年(1994)7月27日

(71)出願人 394012175

正岡 孝一

愛媛県今治市中寺367-2番地

(72)発明者 正岡 孝一

愛媛県今治市中寺367-2番地

(54)【発明の名称】 電子計算機におけるセキュリティ、システム保護を行うソフトウェアの構造及び仕組み

(57)【要約】

【目的】 不正プログラムの動作から、電子計算機ならびにコンピューターシステム、情報ネットワーク全般を保護し、誤動作を防止する。

【構成】 不正プログラムの差分を得、その差分と疑いのあるプログラムを比較することで不正プログラムを発見、除去を行うことで不正プログラムからシステムを保護する。

3 不正プログラム感染の疑いのあるプログラム

2 不正プログラム

【特許請求の範囲】

【請求項1】 電子計算機ウイルス(Computer Virus:コンピュータウイルス)・不正プログラム(オペレータが期待していない動作を行うプログラム)など(以下不正プログラムと、まとめて略す。)が侵入・感染・潜伏(不正プログラムが、既に電子計算機に侵入している)・発病(破壊活動などの表面化される現象)するのを検知・除去・防御する方法として、電子計算機のすべての記憶媒体ならびに、メモリー(記憶装置)におけるプログラムの增量、内容の比較、書き込み動作についての監視を行う。

【請求項2】 不正プログラムが侵入・感染・潜伏・発病するのを検知・除去・防御する方法として、電子計算機の割り込みベクタセットの監視を行う。

【請求項3】 不正プログラムが侵入・感染・潜伏・発病するのを検知・除去・防御の方法として、プログラムファイル・システムファイル・データーファイル(以下ファイルと、まとめて略す。)の名称及び拡張子・内容・日付・サイズが、前回検査した時と変更されていないか監視する。

【請求項4】 不正プログラムが侵入・感染・潜伏・発病するのを検知・除去・防御する方法として、ファイルを削除しようとしていないか、新たなファイルを作成(コピーを含む)しようとしていないか監視する。

【請求項5】 不正プログラムが侵入・感染・潜伏・発病するのを検知・除去・防御する方法として、プログラムがメモリーに常駐したまま処理が終了するのを監視する。

【請求項6】 不正プログラムが侵入・感染・潜伏・発病するのを検知・除去・防御する方法として、アップリケート・ディスク・ライトコマンド(直接記憶媒体にデータを書き込む動作)および、記憶媒体を直接書き込む動作を監視する。

【請求項7】 不正プログラムが侵入・感染・潜伏・発病するのを検知・除去・防御する方法として、不プログラムが持っている特定コードと、その調べようとするプログラムのコードが、似ていないか比較検査を行う。

【請求項8】 不正プログラムが侵入・感染・潜伏・発病するのを検知・除去・防御する方法として、ブートセクタ・IPLのサイズ及び日付、もしくは内容が前回検査した時と変更されていないかチェックを行う。

【請求項9】 不正プログラムが侵入・感染・潜伏・発病するのを検知・除去・防御する方法として、基本ソフトの管理外のセクタ及び使用禁止セクタ、スキップセクタの中に不正プログラムが持っている、特定コードが存在するか比較検査を行う。

【請求項10】 不正プログラムが侵入・感染・潜伏・発病するのを検知・除去・防御する方法として、電子計算機の処理速度の低下を検査する。

【請求項11】 不正プログラムが侵入・感染・潜伏・

発病するのを検知・除去・防御する方法として、システムロックの参照しているプログラムをチェックする。

【請求項12】 不正プログラムが侵入・感染・潜伏・発病するのを検知・除去・防御する方法として、不正プログラムが予測されるプログラムに、プログラム自体が書き変わっているかのどうかの自己診断機能をつけ、もし内容が変更されている場合は、修復・警告メッセージの表示などを行う。

【請求項13】 不正プログラムが侵入・感染・潜伏・発病するのを検知・除去・防御する方法として、不正プログラムに感染したプログラムから検知・除去プログラムを作成する為、ウイルスに故意に用意したプログラムに感染させて、プログラムの差分を得て、その差分とウイルスの感染を疑われているプログラムを、比較する事によってウイルスの検知・除去を行う。

【請求項14】 不正プログラムが侵入・感染・潜伏・発病するのを検知・除去・防御する方法として、不正プログラムから抜き出した差分情報を、不正プログラムの検知プログラムとは別のファイルを作成・参照を行うことによって、新種の不正プログラムが発見された場合、不正プログラムの検知プログラムを書き換えることなく、不正プログラムの参照ファイルだけを差し替えることで新種の不正プログラム対応が可能となる。

【請求項15】 不正プログラムが侵入・感染・潜伏・発病するのを検知・除去・防御する方法として、システムを起動させる時に、あらかじめ用意した不正プログラムの検知プログラムが実行される。このウイルスの検知プログラムは、基本ソフト(オペレーティングシステム)・検知プログラム自体のプログラムのタイムスタンプ・サイズ・内容が変更されていないかチェックを行う。もし変更されている場合は、不正プログラム発見のメッセージ、ならびに不正プログラムを削除などの処置を施す。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は、不正プログラムより電子計算機を保護するソフトウェアの構造及び仕組みに関する。

【0002】

【従来の技術】従来は、不正プログラムが発見されると、人間の手で消していた。

【0003】

【発明が解決しようとする課題】従来においては、不正プログラムが発見されると人間の手で削除していたため、完全に削除できなかったり感染していないものを削除してしまう問題点があった。

【0004】本発明は、電子計算機をより円滑に利用するため、不正プログラムにより電子計算機上の情報の漏洩・破壊などから保護するための、構造及び仕組みを提供することを目的としている。

【0005】

【課題を解決するための手段】上記目的を達成するためには、本発明においては電子計算機に不正プログラムが侵入・感染・潜伏・発病を検知し、除去・防御するソフトウェアである。

【0006】また、新種の不正プログラムに対しても、本システム上で解決するため専門の知識が必要なく利用者自身がすぐ対応できる。

【0007】

【作用】上記のような、ソフトウェアを使用することにより、電子計算機を保護し円滑に利用できる。

【0008】

【実施例】実施例について図面を参照して説明すると、図1において（正常なプログラム）（1）と（不正プログラム）（2）を比較することで不正プログラムに感染した時の差分を得ることが可能である。

【0009】図2において上記の方法から算出した不正プログラムの差分から（不正プログラム感染の疑いのあるプログラム）（3）を比較することで不正プログラムに感染されているか検査が可能である。また感染されている場合は、不正プログラムが感染するのと逆算する方

法で、元の正常なプログラムに修復が可能である。

【0010】

【発明の効果】本発明は、以上説明したように構成されているので、以下に記載されるような効果を奏する。

【0011】不正プログラムの動作から、電子計算機ならびにコンピューターシステム、情報ネットワーク全般を保護することができる。

【0012】そして、コンピューターシステムを保護する事により、記憶メモリーなどが破壊されるのを防ぎ、誤動作を防止できる。

【図面の簡単な説明】

【図1】正常なプログラムと正常なプログラムに不正プログラムが感染したのを示す図である。

【図2】不正プログラム感染の疑いのあるプログラムと図1で示すに計算した不正プログラムから得た差分を比較するのを示す図である。

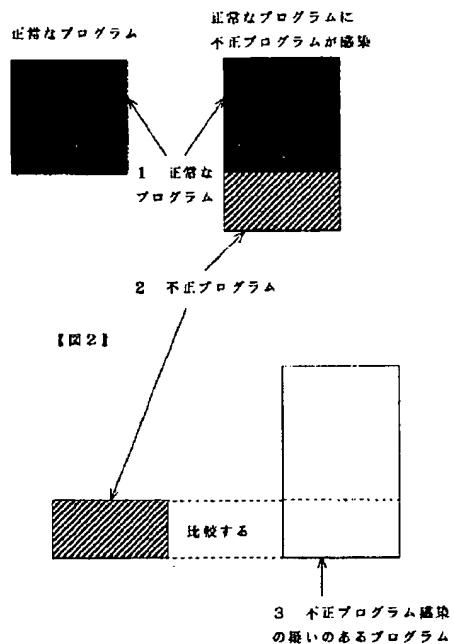
【符号の説明】

1 正常なプログラム

2 不正プログラム

20 3 不正プログラム感染の疑いのあるプログラム

【図1】



【手続補正書】

【提出日】平成6年11月28日

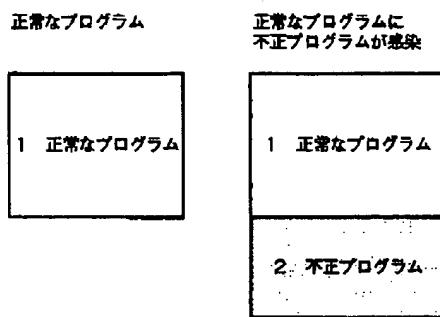
【補正対象書類名】図面

【補正対象項目名】全図

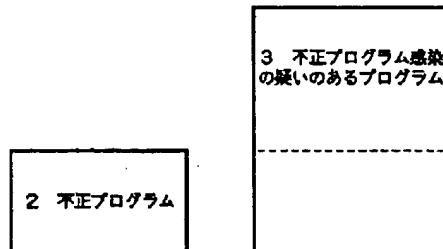
【補正方法】変更

【補正内容】

【図1】



【図2】



DERWENT-ACC-NO: 1996-173962

DERWENT-WEEK: 199618

COPYRIGHT 1999 DERWENT INFORMATION LTD

TITLE: Software for protecting electronic
computer from inaccurate program and computer virus
- detects invalid program by comparing inaccurate
program with program with doubt of inaccurate program infection

----- KWIC -----

Basic Abstract Text - ABTX (1):

The software involves the omission of an inaccurate program, computer virus which enters the memory of an electronic computer. The inaccurate program performs inaccurate operation which are not expected by the user by monitoring the write-in operation and comparing the inaccurate program (2) with program (3) with doubt of inaccurate program infection. The inaccurate program is identified and removed.

Derwent Accession Number - NRAN (1):
1996-173962

Title - TIX (1):

Software for protecting electronic computer from inaccurate program and computer virus - detects invalid program by comparing inaccurate program with program with doubt of inaccurate program infection

Standard Title Terms - TTX (1):

SOFTWARE PROTECT ELECTRONIC COMPUTER INACCURACIES
PROGRAM COMPUTER VIRUS
DETECT INVALID PROGRAM COMPARE INACCURACIES PROGRAM PROGRAM
INACCURACIES

PROGRAM INFECT